Formal Proof of Banach-Tarski Paradox

Daniel de Rauglaudre

Formal Proof of Banach-Tarski Paradox

DANIEL DE RAUGLAUDRE
INRIA Paris, France

Banach-Tarski Paradox states that a ball in 3D space is equidecomposable with twice itself, i.e. we can break a ball into a finite number of pieces, and with these pieces, build two balls having the same size as the initial ball. This strange result is actually a Theorem which was proven in 1924 by Stefan Banach and Alfred Tarski using the Axiom of Choice.
We present here a formal proof in Coq of this theorem.

1. INTRODUCTION

Mathematical books and papers often contain errors which are sometimes very difficult to detect, particularly when the mathematical topics are complicated and when few people understand them. Formal proofs are answers to these questions because they allow to verify proofs, to be sure they do not contain errors. They also enlarge the set of mathematicians who can accept the proofs because all details are required by the proof assistant software.

Moreover, formal proofs allow to know exactly which axioms are required, if any. In the case of Banach-Tarski Paradox, it is well known that the Axiom of Choice is used. The formal proof shows exactly when and how this axiom is used.

This paper describes a translation of Banach-Tarski Paradox into Coq [Tea17]. After a preliminary remark about *sets*, we remind the sketch of the proof of Banach-Tarski Paradox. Then we give some aspects encountered in the Coq proof.

2. PRELIMINARY REMARK

This paper will often use the term *set*. Actually, these sets are not the ones of ZF, because Coq is not based on set theory but on type theory. What we call "sets" here are actually subsets, i.e. subtypes, i.e. predicates on a type. Since the theorem describes objects in $\mathbb{R}^3$, our sets will be predicates on a point type (triplet of reals), i.e. functions taking a point and returning a value telling if the point is or is not in the set. It is possible to easily define membership, union, intersection, subtraction, inclusion, equality. See Section 4.1

3. SKETCH OF THE PROOF

We explain here the proof as it is usually described[1]. We often say "we" in this section to describe the proof, but it is not "our" work. The proof already exists and we just make a formal version of it. Our real work, the translation of the proof into Coq, is explained in the next section.

Roughly speaking, two geometric objects are *equidecomposable* if we can take one object, break it into a finite number of pieces, and then build the second object with them.

[1] Banach-Tarski paradox — Wikipedia, the free encyclopedia,2017. [Online; accessed 16-Apr-2017].

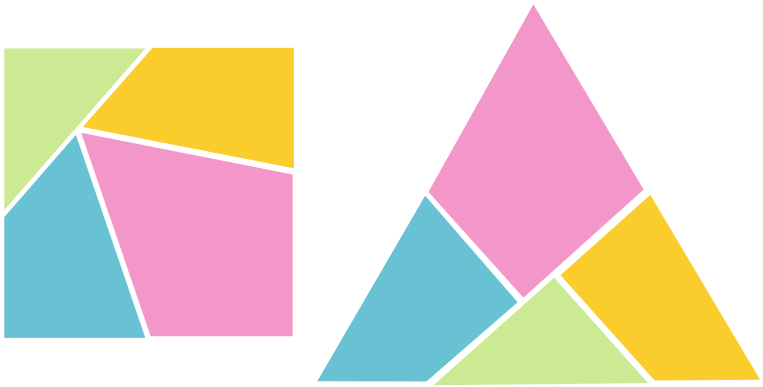

Fig. 1. Equidecomposability (image Wikipedia)

In mathematical terms, two geometric objects (as sets of points) are equidecomposable if there exists a partition of the first set and a partition of the second set, such that each part of the first partition is mapped to a part of the second partition by translations and rotations. The two partitions have therefore the same number of parts. The number of parts in the partitions must be finite.

So it seems strange that a ball can be broken into pieces and that we are able to build, with these pieces, two balls of the same size as the initial ball!

This is due to the fact that, when the Axiom of Choice is used, it is possible to build objects that are not measurable. This is what happens in this theorem (even if this consideration is actually not required in the proof).

3.1 Principle of the Proof

We first consider the ball without its center. Indeed, a ball (set of all points whose distance to origin is not greater than 1) can be seen as an infinity of spheres (set of all points whose distance to origin is constant), but the theorems about them do not work for spheres of radius 0. The inclusion of the center is treated afterwards.

In the following, we refer to spheres, noted S^2 (implicitely depending on a radius r), but since it is for any non zero radius, the same reasonings apply to balls (noted B) of radius not greater than 1 and without its center (noted C).

A first version of the proof shows that we can break the first sphere, build two spheres and get an extra piece, unused. In the final version, this extra piece can be included in one of the parts by means of some refinements.

In the first version, we break the initial sphere into five parts: with two parts, we can build a sphere, with two other parts, another sphere. The ways the two spheres are built are identical. The fifth part is remaining: it is the extra piece. We show how to include this extra piece later.

3.2 Angle

In order to make the partition of the sphere, we first start by choosing an angle. Any angle is suitable, provided it is not a rational multiple of π. The idea is that, when we rotate the sphere with this angle, one or several times, possibly a countable

infinity number of times, no point is mapped to itself, except the two points on the rotation axis.

For practical reasons, in the pen-and-paper proof, the chosen angle is $acos(1/3)$ which is indeed not a rational multiple of π.

We then consider all sequences of rotations of the sphere, 1) around the x axis and 2) around the z axis (only these two axes, not the y axis), all rotations being of angle $acos(1/3)$. By abuse of notation, we respectively name x and x^{-1} these rotations around the x axis in one direction and the opposite, z and z^{-1}, these rotations around the z axis. So a sequence of rotations can be represented as a string of x, x^{-1}, z, z^{-1}.

3.3 Orbit

Let us take a point on the sphere, any point. From that point, any string of x, x^{-1}, z, z^{-1} determines a *path* of rotations, mapping the initial point to another point on the sphere. Going through all possible paths, we get a set of points which is called the *orbit* of the point. We then fill the sphere with a countable number of point, therefore not the whole sphere which has an uncountable number of points.

3.4 Using the Axiom of Choice

We now want to cover the whole sphere with all possible orbits. Since the number of points in an orbit is countable, there is an uncountable amount of orbits. However there is no direct way to find them. To do it, we need the Axiom of Choice.

The version of Axiom of Choice used takes a set and an equivalence relation on this set and returns a function which, for each element of the set returns a representative of the equivalence class it belongs to. For a given equivalence class, the representative is unique: for two elements of the same class, the returned value of the function is the same.

Being on the same orbit is trivially an equivalence relation. Using the above version of the Axiom of Choice, we can get all orbits covering the sphere: the image of the choice function gives us representatives of all orbits of the sphere and only them.

3.5 Partitions of Orbits

When we take one orbit, we distinguish five sets of points:

—the initial point
—all points whose paths end with x
—all points whose paths end with x^{-1}
—all points whose paths end with z
—all points whose paths end with z^{-1}

A precision: paths we are talking about are *normalized* paths, i.e. not containing sequences xx^{-1}, $x^{-1}x$, zz^{-1}, $z^{-1}z$ which cancel themselves.

The union of these sets is equal to the orbit of the initial point.

Actually, in some kinds of orbits, some points may appear several times. For example, if we start from the point $(1, 0, 0)$, which is on the x axis, rotations x or x^{-1} obviously do not move this point. Therefore, this point belongs to the first

three sets above at the same time. However, starting with a rotation z or z^{-1} it can be proven that we never return to the point $(1, 0, 0)$: this proof is made easier by using a useful property of the angle $acos(1/3)$.

This problem can be generalized to any path of rotations of x, x^{-1}, z, z^{-1}. Since a product of rotations is a rotation, a given path of these rotations has two fixed points, p and its opposite $-p$. The orbit of p (and $-p$) has the same problem as $(1, 0, 0)$ above: when going through its orbit, the given path maps p to itself. So, the five sets of points above do not partition the orbit of p, since p belongs to the first set, and to the set ending with the ending rotation of the given path.

3.6 The set D

There is a countable number of paths, therefore a countable number of orbits holding a fixed point, so a countable number of points belonging to an orbit holding a fixed point. We name this set D. It can be proven that D is the only set of points on the sphere which belong to orbits holding a fixed point. If we (temporarily) discard D, all orbits contain points that are all different and different from the points of the other orbits. The five sets above form a true partition of the set of their orbits.

We are now proving Banach-Tarski on $B \setminus D$ (and without the center, but we do not need to take that into account, because the center actually belongs do D). The problem of including D is treated after.

3.7 Partition of the Sphere

Going through all orbits but D, we group together all the five sets, one by one. We get:

(1) the set M of all initial points,
(2) the set $S(x)$ of points whose path from the initial point ends with x,
(3) the set $S(x^{-1})$ of points whose path from the initial point ends with x^{-1},
(4) the set $S(z)$ of points whose path from the initial point ends with z,
(5) the set $S(z^{-1})$ of points whose path from the initial point ends with z^{-1}.

The set M contains all representatives of each orbit, it is the image of the choice function. The five sets make a partition of the sphere (minus D).

With the sets 2 and 3 above, we can build a sphere (but D). This is the central point of the proof.

Indeed, we take the set 2 without change, and we rotate the set 3 with an extra x. This extra x cancels with the ending x^{-1}. This rotated set then contains:

—all points with en empty path (set 1) if the initial path was just x^{-1},
—all points whose path ends with x^{-1} (set 3) if the initial path ended with $x^{-1}x^{-1}$,
—all points whose path ends with z (set 4) if the initial path ended with zx^{-1},
—all points whose path ends with z^{-1} (set 5) if the initial path ended with $z^{-1}x^{-1}$.

And only them. It does not contain the set 2 since the paths of the set 3 cannot end with xx^{-1} which would have cancelled themselves. So the rotated set 3 is a complement of the set 2.

Therefore, the set 2 and the rotated set 3 form a partition of the sphere but D. Doing the same thing with the sets 4 and 5, we get another sphere but D. The set 1, M, is an extra piece.

3.8 Including the extra Piece

We now add the set M into the set $S(x)$ (Section 3.7). So, the partition of the sphere but D becomes:

—$S(x) \cup M$
—$S(x^{-1})$
—$S(z)$
—$S(z^{-1})$

But if we apply the recipe of the previous section, it does not work because the set M appears twice: $1/$ in $S(x) \cup M$ not rotated and $2/$ in $S(x^{-1})$ rotated with x. To resolve that, the proof considers the set G defined as:

$$G = x^{-1}M \cup x^{-2}M \cup x^{-3}M \cup ...$$

and we add it to the first set and subtract it from the second set. The four sets become:

—$A_1 = S(x) \cup M \cup G$
—$A_2 = S(x^{-1}) \setminus G$
—$A_3 = S(z)$
—$A_4 = S(z^{-1})$

Now, since $xG = M \cup G$, when we rotate A_2 with x, M disappears from this second set and we can say that A_1 and xA_2 form a partition of the sphere. We then get our two spheres but D without an extra piece.

3.9 Including D

We have now Banach-Tarski on the ball without center nor D: it is equidecomposable with twice itself. Equidecomposability being an equivalence relation, if we prove that the sphere is equidecomposable with a sphere but D, we have Banach-Tarski on balls but centers.

For that, the proof uses Hilbert's Hotel trick[2]. We start with a sphere without D. We rotate it so that the points in D are filled by points further, we fill these new points by the points still further, and so on, up to infinity. At the end, all points of the sphere are filled. Actually we do all of that using equidecomposability. We are going to explain how in the following.

First, for a rotation that is going to be applied later, we take an axis whose two intersections with the sphere do not belong to D: these points do exist since D has a countable number of points but the sphere has an uncountable number of points.

Second, we find a rotation angle having good properties. For that, we consider the set J_0 of all rotations around the chosen axis which map at least one point of

[2]Hilbert's paradox of the grand hotel — Wikipedia, the free encyclopedia, 2017. [Online; accessed 17-Apr-2017].

D to a point of D. Since D is countable, the set J_0 contains at most a countable number of rotations.

Then we consider the set J of all rotations whose angles are integer divisors of angles of rotation in J_0. For example, if J_0 contains the angle α, J will contain the angles α, $\alpha/2$, $\alpha/3$, etc. And also modulo 2π, i.e. $(\alpha + 2\pi)/2$, $(\alpha + 2\pi)/3$, $(\alpha + 4\pi)/3$, $(\alpha + 2\pi)/4$, ...

J is obviously at most countable. Therefore, since there are an uncountable number of rotations around the chosen axis, there must exist a rotation not in J. We name this rotation ρ.

By definition of ρ, for all natural numbers n, no point of D rotated with ρ^n is mapped to another point of D. Let us define the set E as:

$$E = D \cup \rho D \cup \rho^2 D \cup \rho^3 D \cup ...$$

We remark that $\rho E = E \setminus D$. We can then prove that the sphere and the sphere but D are equidecomposable: indeed, the sphere (S^2) can be partitioned with E and $S^2 \setminus E$, and the sphere but D can be partitioned with ρE and $S^2 \setminus E$. The second partitioning is derived from the first one with rotation ρ for the first part and identity for the second part. The two sets are therefore equidecomposable.

3.10 Including the Center

The ball without its center is trivially equidecomposable with the ball without the point on the x axis $(1, 0, 0)$. Then we apply the Hilbert's Hotel trick once again by rotating the ball by z: we know that no point maps to itself, even rotating several times. We note G the set holding the singleton point $(1, 0, 0)$ and we consider the set F defined as:

$$F = G \cup zG \cup z^2 G \cup z^3 G \cup ...$$

Since $zF = F \setminus G$, we can partition $B \setminus G$ with zF and $B \setminus F$ and partition the ball with F and $B \setminus F$, which make them equidecomposable. □

4. COQ PROOF

We present here the formal proof, i.e. the translation of this proof into Coq.

In the following, the displayed code, when any, is not real Coq code, but rather *pseudo-code* holding simplifications to make it easier to read and understand.

4.1 Representation of Sets

As we said in Section 2, our sets are not the ones defined by ZF. They are just defined as predicates on a parameter type A, included in a record type to distinguish from other predicates:

Record set A := mkset { setp : A → Prop }.

We define the classical notation for membership with:

Notation "x ∈ S" := (setp S x) (at level 60).

So empty set, union, intersection, subtraction, inclusion, equality can be easily defined:

$\emptyset :=$ mkset $(\lambda x, False)$
$S_1 \cup S_2 :=$ mkset $(\lambda$ x, x $\in S_1 \vee$ x $\in S_2)$
$S_1 \cap S_2 :=$ mkset $(\lambda$ x, x $\in S_1 \wedge$ x $\in S_2)$
$S_1 \setminus S_2 :=$ mkset $(\lambda$ x, x $\in S_1 \wedge$ x $\notin S_2)$
$S_1 \subset S_2 := \forall$ x, (x $\in S_1 \rightarrow$ x $\in S_2)$
$S_1 = S_2 := \forall$ x, (x $\in S_1 \leftrightarrow \in S_2)$

4.2 Decidability of Membership

In several places of the proof, we need the decidability[3] of membership, i.e. that for any set S and any element x, we are allowed to say: either $x \in S$ or $x \notin S$. This can be achieved by the Axiom of Excluded Middle. But since the proof uses the Axiom of Choice which implies the Excluded Middle (see Section 4.4), we get here the Excluded Middle as a theorem.

The places where we need the decidability of membership are the following:

—When including the "extra piece" M (Section 3.8), we needed to prove that if S_1, S_2 ... form a partition of S, and that S'_2 is a subset of S_2, then $S_1 \cup S'_2$, $S_2 \setminus S'_2$ ... also form a partition of S. The proof requires the decidability of membership in S'_2. This theorem is applied with $S = B \setminus D$, $S_1 = M \cup S(x)$, $S_2 = S(x^{-1})$, $S'_2 = G$, the remaining sets on the list being $S(z)$ and $S(z^{-1})$.

—We used several times the fact that if S_1 is a subset of S, then S_1 and $S \setminus S_1$ form a partition of S. This is a corollary of the previous theorem, but it was proved independently for practical purposes (the proof that it is a corollary required an extra property which was complicated to prove). For the same reason, the decidability of membership to S_1 is required in the proof. This theorem is used:
  —when proving that $B \setminus C \setminus D$ and $B \setminus C$ are equidecomposable.
  —when proving that $B \setminus C$ and $B \setminus (1,0,0)$ are equidecomposable,
  —when proving that $B \setminus (1,0,0)$ and B are equidecomposable,

—When proving that $(E \setminus D) \cup (B \setminus C \setminus E) = B \setminus C \setminus D$, we need the decidability of membership in E.

4.3 Transitivity of Equidecomposability

While proving that equidecomposability is an equivalence relation, the proof that it is transitive was a little bit tricky. Because when two sets are equidecomposable, the way they are so depends on the existence of partitions with the same number of parts.

But in transitivity, the intermediate set is partitioned twice: once with the first set, and once with the third set. And there is no reason that the two partitions of this second set would be identical. Even the number of parts can be different.

We must then make the intersection of the two partitions and apply the transformations or their inverses to get a partition of the first set and a partition of the third set having the same number of parts, and compute the transformations from one to the other.

It took us one month to achieve the translation of this part of the proof into Coq.

[3] The term *decidability* generally means that there is an algorithm able to determine if a proposition is true or false. Here, we use *decidability* in a weaker meaning: we allow ourselves to say that either a proposition holds or its contrary holds, even if we don't have an algorithm computing it.

4.4 Axiom of Choice

A version of this axiom, named TTCA (Type Theoretical Axiom of Choice) [Wer97] says that if we have an equivalence relation (here, being in the same orbit), we can have a function taking an element and returning a representative of the equivalence class it belongs to. Namely:

$$\begin{array}{l} \forall\ R\ (\mathit{equivalence\ relation})\ \exists\ f \\ \quad \forall\ x \quad R(x, f(x)) \quad \wedge \\ \quad \forall\ x\ \forall\ y \quad R(x,y) \Rightarrow f(x) = f(y) \end{array}$$

Notice that the last line of this definition says that the representative of an equivalence class is unique.

The name "TTCA" comes the paper above, but in in the next version of Coq (8.7), this axiom was added and named "SetoidFunctionalChoice", which emphasizes the fact that it is a version of the Axiom of Choice based on *setoids*, i.e. sets associated with equivalence relations. AC indeed needs, as hypothesis, a family of (non empty) sets: but Set Theory does not see a difference between a family of sets and a set with an equivalence relation (and its classes). Here, a definition of the axiom with just a family of sets would not work, because we do not know how to build these sets: we just have an equivalence relation and no way to know where its equivalence classes are. Indeed, when we create an orbit of one point, it is impossible to create an orbit of another point that we can be sure it is not in the orbit of the previous point: there is no criterion to know it and no algorithm which would answer this question in a finite time. Therefore we needed a version of AC which provided not only the choice function but also the required family of sets (the equivalence classes).

More about the axiom of choice in type theory can be found here [Bel15].

This version of the Axiom of Choice implies the Excluded Middle [Dia75]. The proof is relatively simple[4]. Then we have Excluded Middle as a theorem, and this is used in the proof several times (decidability of membership, Section 4.2).

4.5 Rotations and Matrices

Rotations can be represented in two ways:

(1) either by the pair (axis, angle),
(2) or by matrices of determinant 1, inverse of their transpose.

The first way seems more intuitive, but the second way is easier to manipulate: it does not require the use of the constant π, the functions sinus, cosinus, trigonometric formulas and so on. So we chosed this second implementation.

Nevertheless, conversion from matrix to axis and angle was required here and there in the proof (Section 4.9).

4.6 Orbit of Point (1,0,0)

Using the fact that the chosen angle is $acos(1/3)$, it is possible to prove that when starting a path with a rotation z or z^{-1} (i.e. around the z axis), it is impossible for the point $(1, 0, 0)$ to return to itself. This result is used in two parts of the proof:

[4] Diaconescu's theorem — Wikipedia, the free encyclopedia, 2017. [Online; accessed 20-Apr-2017].

—first, together with the same proof with $(0,0,1)$, it can be proven that a non empty path cannot be the identity rotation,

—second, when proving that the ball but the center is equidecomposable with the whole ball, it is used when the center is moved to the point $(1,0,0)$ and the point $(1,0,0)$ is moved an infinity of times by a rotation around the z axis. We use a rotation of $acos(1/3)$ for that.

The first point above is required to prove that the set D is countable.

4.7 Proof that D is countable

From the point of view of a mathematician, it is obvious that D is countable. Indeed, to build D, we consider all paths made of x, x^{-1}, z, z^{-1} which are countable, all fixed points of the rotations defined by these paths (two by rotation), and all orbits of these fixed points, also countable since orbits are also built by paths. D is the set of all points of these orbits. Therefore D is countable.

In the details, things are not so simple: we had to ensure that no path leads to the identity rotation. Indeed, in the identity rotation, all points are fixed points and, in that case, the set D would not be countable. The previous section told us that this point has been proven.

There is also something particular for the rotation by π. Indeed, the fixed points being the axis of rotation, we must find the rotation axis from the rotation matrix. Unfortunately, the very simple formula that gives us the rotation axis from the matrix, which is, in the general case, the following vector:

$$\begin{pmatrix} a_{1,2} - a_{2,1} \\ a_{2,3} - a_{3,2} \\ a_{3,1} - a_{1,3} \end{pmatrix}$$

does not work for rotation by π: it becomes the zero vector. Some methods exist to get the rotation axis when the angle is π, but they are complicated and it is hard to prove their properties.

Fortunately, there is a very simple solution of this problem: actually, it is easy to see that a non empty path cannot be a rotation by π: if it were, concatenating the path with itself would generate the identity rotation, which is impossible since we proved that no empty path can be the identity rotation.

Even though the resulting formalized proof is relatively simple, we took about one month to complete it, to understand the good way to do it.

4.8 Proof that J is countable

J_0 (Section 3.9) is the set of all rotations around the chosen axis which map at least one point of D to a point of D. Since D is countable, all pairs of points of D are countable. J_0 contains the ones which are on the same latitude on the sphere (the axis going through the north and south poles). It is a subset of a countable set, therefore countable.

J is the set of all integer divisors n of the rotation angles of J_0, modulo $2k\pi$. Since pairs of integers (n,k) are countable, it it still countable.

4.9 Angles as pairs (sin, cos)

In most of the proof, we often use the pair (s, c) for angles and a proof that $s^2 + c^2 = 1$, supposed to represent a sinus and a cosinus, instead of the angles themselves. This idea came from the formula that gives the rotation matrix. We remark that this formula only depends on the axis (x, y, z) and on the sinus s and the cosinus c of the angle. The rotation matrix is (in pseudo-code):

Definition `matrix_of_axis_angle((x,y,z),s,c)` :=
`(x`^{2}`(1-c)+c)` `(xy(1-c)-zs)` `(xz(1-c)+ys)`
`(xy(1-c)+zs)` `(y`^{2}`(1-c)+c)` `(yz(1-c)-xs)`
`(xz(1-c)-ys)` `(yz(1-c)+xs)` `(z`^{2}`(1-c)+c).`

So representing angles with s, c and a proof that $s^2 + c^2 = 1$, we can make rotation matrices and we do not need to worry about π and reasoning modulo 2π: therefore, representations of angles are unique. This way, we can rotate points of the sphere by matrix-vector multiplications, combine rotations by multiplying matrices, and reverse rotations.

Nevertheless, in some cases, we need the rotation angle. We can get an angle between 0 and 2π from the pair (s, c) by the following function:

Definition `angle_of_sin_cos(s,c)` :=
  if `s < 0` **then**
    if `c < 0` **then** 2π`-acos(c)` **else** `asin(s)+`2π
  else
    if `c < 0` **then** `acos(c)` **else** `asin(s)`.

Notice that in the used version of Coq, the functions *asin* and *acos* were missing. So we defined them as:

Definition `asin(x)` := `atan'(x,`$\sqrt{}$`(1-x`^{2}`)).`
Definition `acos(x)` := π`/2-asin(x).`

where

Definition `atan'(x,y)` := **if** `y = 0` **then** `sign(x)`π`/2` **else** `atan(x/y).`

where `sign(x)` is -1 if x is negative, or 1 if x is positive.

We proved in Coq that, for all `x s c`,

— `angle_of_sin_cos(sin(x),cos(x)) = x modulo` 2π,
— `sin (angle_of_sin_cos s c) = s`,
— `cos (angle_of_sin_cos s c) = c`,
— providing that `v` is not the empty vector, and $s^2 + c^2 = 1$, the result of `matrix_of_axis_angle(v,s,c)` is indeed a rotation matrix (its determinant is 1 and the product with its transpose is the identity matrix).

All these definitions and theorems could be added as a new library in Coq.

The conversion from (s, c) to angles is used first in the proof that J is countable (Section 4.8), because we need to find the pair of sinus and cosinus for angles divided by natural numbers.

Then it is used for the proof that $\rho E = E \setminus D$ (Section 3.9). For it, we need to prove that if a point p belongs to D and is equal to $\rho p'$ where p' belongs to D too, then ρ is in J (contradiction).

To find all angles of J, we need actually to take all angles of J_0 modulo $2k\pi$ divided by an integer. So we need to take care of sinus and cosinus of angles of the form $(\theta + 2k\pi)/n$. It is the reason why we needed theorems involving $asin$ and $acos$.

4.10 Nsatz

The Coq tactic `nsatz` has been used several times. In these cases, this tactics seemed to be the only solution to resolve the involved goals. But we are not fully satisfied by this necessity: it could have been interesting to know how this tactic managed to find its solutions and be able to do them by hand, if we wanted. For us, `nsatz` sounds a little bit like "magic".

We used it in the following situations:

—when proving that the product of two matrices built from a common axis and two angles is equal to the matrix built from the axis and the sum of the angles,

—when proving that if a point in on the sphere, any rotation of the sphere maps this point to another point still on the sphere (obvious, but had to be formally proved),

—when proving that if a point is on a rotation axis, the product of this rotation matrix with the point is equal to this point,

—when proving that the product of a rotation matrix to a cross product of two vectors is the cross product of the product of the matrix to each vector,

—when proving that if the cross product of two vectors having the same norm is equal to zero, then either these vectors are equal or they are opposite,

—when proving that if the dot product of two vectors having the same norm is equal to one, then these vectors are equal,

—when proving that a rotation matrix maps a point to another point which is on the same latitude (considering that the rotation axis goes through the north and the south poles),

—and in another case of a lemma involving matrices and a function converting three vectors to the pair of the sinus and the cosinus of the angle they form.

5. AXIOMS USED

The only axiom explicitely used in the proof is the Axiom of Choice (TTCA). The coq command "`Print Assumptions Banach_Tarski_paradox`" answers:

```
Axioms:
up : ℝ → ℤ
total_order_T : ∀ r1 r2 : ℝ, r1 < r2 + r1 = r2 + r1 > r2
```

```
completeness : ∀ E : ℝ → Prop, bound E → (∃ x : ℝ, E x) → {m : ℝ | is_lub E m}
Classical_Prop.classic : ∀ P : Prop, P ∨ ¬ P
archimed : ∀ r : ℝ, IZR (up r) > r ∧ IZR (up r) - r ≤ 1
TTCA : ∀ (A : Type) (R : A → A → Prop),
  equiv A R
  → ∃ f : A → A, (∀ x : A, R x (f x)) ∧ (∀ x y : A, R x y → f x = f y)
Rplus_opp_r : ∀ r : ℝ, r + - r = 0
Rplus_lt_compat_l : ∀ r r1 r2 : ℝ, r1 < r2 → r + r1 < r + r2
Rplus_comm : ∀ r1 r2 : ℝ, r1 + r2 = r2 + r1
Rplus_assoc : ∀ r1 r2 r3 : ℝ, r1 + r2 + r3 = r1 + (r2 + r3)
Rplus_0_l : ∀ r : ℝ, 0 + r = r
Rplus : ℝ → ℝ → ℝ
Ropp : ℝ → ℝ
Rmult_plus_distr_l : ∀ r1 r2 r3 : ℝ, r1 * (r2 + r3) = r1 * r2 + r1 * r3
Rmult_lt_compat_l : ∀ r r1 r2 : ℝ, 0 < r → r1 < r2 → r * r1 < r * r2
Rmult_comm : ∀ r1 r2 : ℝ, r1 * r2 = r2 * r1
Rmult_assoc : ∀ r1 r2 r3 : ℝ, r1 * r2 * r3 = r1 * (r2 * r3)
Rmult_1_l : ∀ r : ℝ, 1 * r = r
Rmult : ℝ → ℝ → ℝ
Rlt_trans : ∀ r1 r2 r3 : ℝ, r1 < r2 → r2 < r3 → r1 < r3
Rlt_asym : ∀ r1 r2 : ℝ, r1 < r2 → ¬ r2 < r1
Rlt : ℝ → ℝ → Prop
Rinv_l : ∀ r : ℝ, r ≠ 0 → / r * r = 1
Rinv : ℝ → ℝ
R1_neq_R0 : 1 ≠ 0
R1 : ℝ
R0 : ℝ
R : Set
```

We indeed see TTCA. The other axioms come from the Coq library on real numbers. We notice that the Excluded Middle (Classical_Prop.classic) is present, likely used by theorems or definitions in the Coq library on real numbers. We do not explicitely use it in the proof, rather using its equivalent as a corollary of the Axiom of Choice (Section 4.4).

6. CONCLUSION

This is the first formalized proof of Banach-Tarski Paradox, a new contribution to the formalization of mathematics. Our aim was to try to understand its proof in depth, to find which axioms are required and why. It is one of the reasons why few automations were used.

Formalization of mathematical proofs is often long, hard, and require much patience. It is not especially due to Coq, but rather to mathematical sub-problems generated by the problem itself, by details that mathematicians consider as obvious, but which are often tedious to formalize. For example, here, the proofs that the sets D and J (see 4.7 and 4.8) are "obviously" countable, from an intuitive geometric point view, are not so simple to formalize.

Some results used in the proof are worth being integrated to a standard library: Cauchy-Schwarz inequality, representation of angles with pair (sin,cos), uncountability of $\mathbb{R}$, definition and properties of asin and acos.

It took nine months (265 days exactly) to achieve the proof (one person), from 20th of July 2016 to 11th of April 2017 at 11:08 a.m. Paris time.

The final Coq code has around 11,000 lines. It was initially compiled with Coq version 8.6 [Tea17]. It uses only the Coq Libraries (no other libraries or extensions).

The code is accessible at `https://github.com/roglo/banach_tarski`.

ACKNOWLEDGMENT

Some colleagues helped for mathematical issues, advices on Coq and reading the present paper: Théo Zimmerman, Hugo Herbelin, Rémi Nollet, Maxime Lucas, Cyrille Chenavier, Théo Winterhalter and some others. Thanks to them.

References

[Bel15] John L. Bell. The axiom of choice. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, summer 2015 edition, 2015.

[Dia75] Radu Diaconescu. Axiom of choice and complementation. *Proceedings of the American Mathematical Society*, 51(1):176–178, 1975.

[Tea17] The Coq Development Team. *The Coq proof assistant reference manual*. PiR2 Team, 2017. Version 8.6.

[Wag93] Stan Wagon. *The Banach-Tarski Paradox*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1993.

[Wer97] Benjamin Werner. Sets in types, types in sets. In *TACS*, volume 1281 of *Lecture Notes in Computer Science*, pages 530–346. Springer, 1997.